REMARKS

In view of the following remarks, Applicant respectfully requests consideration and allowance of the subject application. This amendment is believed to be fully responsive to all issues raised in the 02/13/2006 Office Action.

In the Claims:

No claims are added.

Claims 3, 6, 8, 12 and 16 are original.

Claims 1, 5, 7, 11, 15 and 17—19 are currently amended.

Claim 4 was previously presented.

Claims 2, 9, 10, 13 and 14 were previously cancelled.

Accordingly, claims 1 and 3—8, 11—12, 15—19 are pending.

Traversal of the §103 Rejections

Claims 1, 3, 6—8, 12 and 16—17 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,623,637, hereafter "Jones" in view of U.S. Patent No. 6,178,507, hereinafter "Vanstone." The Applicants respectfully traverse the rejection and request that the rejection be reconsidered and withdrawn.

Claim 1 recites a system for porting user data from one computer to another comprising:

- a memory device configured to store the user data and a public key; and
- a smart card associated with a user that alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when the smart card is absent;
- **wherein the public key is sent from the memory device to the smart card**, wherein the smart card contains a private key, and wherein access to the user data in the memory device **is enabled upon verification that the public key and the private key are associated as a public/private key pair** such that the public and private key are components of an asymmetric cryptographic system

whereby data encrypted by the public key may be decrypted by the private key; and

- wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

The Jones reference does not teach or suggest elements recited by Claim 1. In particular, Jones fails to teach or suggest that, "the public key is sent from the memory device to the smart card". Instead, Jones teaches that and RSA or similar encryption scheme can be used to allow the secure card 400 communicate with a remote computer 450 (see Fig. 3). In particular, Jones teaches that a public key 455 on a remote computer 450 can send an encrypted message to be decoded by a private key 430 on the secure card 400 (see Jones, column 9, lines 26—32). Jones also teaches that data can be sent in the reverse direction, encrypted by the public key 435 on the secure card 400 for transmission to the remote computer 450 where it is decoded by the private key 460 (see Jones, column 9, lines 38—42). Therefore, while Jones does teach aspects of public/private key utilization, *Jones does not teach or suggest a verification scheme wherein the public key is sent to the location wherein the associated private key is located, and particularly where that location is a smart card.* In particular, Jones fails to teach a verification scheme wherein, "the public key is sent from the memory device to the smart card".

The Patent Office acknowledged that Jones does not disclose enablement of a memory device upon verification that the public key and the private key are associated. In response, the Patent Office cited the Vanstone reference as a reference that teaches aspects of authenticity verification using public and private keys.

However, Vanstone fails to teach a verification scheme wherein, "the public key is sent from the memory device to the smart card". Instead, Vanstone teaches that a smart card and a terminal can mutually verify each other using a two-step process, wherein the bulk of the required processing power is borne by the terminal, and the smart card is given less demanding calculations. In particular, the terminal signs information using an RSA algorithm, which is verified by the smart card. Thus, the terminal sends to the smart card information 116 (see Figure 1b) that has been signed by an RSA algorithm. The smart card signs information using an ECC (elliptical curve calculation) algorithm, which is verified by the terminal. Thus, the smart card sends to the terminal information 122 (see Figure 1b) that has been signed by an ECC algorithm. Therefore, it can be seen that Vanstone teaches that the combination of RSA and ECC provide security without overwhelming the calculating power of the smartcard. Therefore, while Vanstone does teach aspects of verification, *Vanstone does not teach or suggest a verification scheme wherein the public key is sent to the location wherein the associated private key is located.* In particular, Vanstone fails to teach a verification scheme wherein, "the public key is sent from the memory device to the smart card".

The Patent Office has not specifically suggested that either Jones or Vanstone teach or suggest that, "the public key is sent from the memory device to the smart card". However, in the rejection of Claims 18 and 19 the Patent Office suggests that the Sigbjornsen reference teaches transfer of an asymmetric key to a smart card. However, as seen in the traversal of the rejection of Claims 18 and 19, Sigbjornsen does not teach or suggest sending the public key "from the memory device to the smart card, wherein the smart card contains a private key, and

wherein access to the user data in the memory device is enabled *upon verification that the public key and the private key are associated as a public/private key pair*". In fact, as will be seen in the discussion of Claims 18 and 19, Sigbjornsen teaches that an asymmetric key can be sent to a smart card in an encrypted state, and that a private key can decrypt the encrypted key. However, no association between the decrypted asymmetric key and the private key is taught as part of an authentication procedure. For a more complete discussion of these issues, the traversal of the rejections to Claims 18 and 19 are incorporated herein by reference. In view of these arguments, it can be seen that Claim 1 recites elements not taught or suggested by the references of record. Because the combined prior art references do not teach or suggest all the limitations of Claim 1 as amended, the rejection is improper. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). The Applicant respectfully requests that the rejection be removed.

Claim 1 has additionally been amended to recite, "wherein the smart card is configured to pass a encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device". Encryption and decryption of the data in the memory device is supported by the Applicant's specification as encryption key 120 (Fig. 3) and at the top of page 12 of the specification, and other locations. The Jones reference fails to teach or suggest such an encryption strategy. Instead, the Jones teaches that he common memory array 150 is unprotected by any encryption key passed from the smart card to the memory device. Similarly, Vanstone teaches a data card verification system, but does not teach the transfer of an encryption key from the smart card to a memory device for decrypting data read from, and encrypting data written to, the memory device. And further, Sigbjornsen also fails to provide

such a teaching. The Patent Office has cited this art for other purposes, and has not asserted that the art discloses the above recited elements. Accordingly, Claim 1 is additionally allowable over the prior art of record for these additional reasons.

Claims 3—5 depend from Claim 1, and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features that, in combination with those recited in the corresponding base claim, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claim 7 recites a computer system, comprising:

- a computer having an interface; and
- a profile carrier adapted to use the interface, the profile carrier comprising a smart card associated with a user and containing a private key and a memory device having data memory to store a user's profile and to store a public key associated with the private key such that the public and private key form a public/private key pair, wherein the smart card alternately enables access to the user's profile when present and disables access to the user's profile when absent;
- wherein the system is configured **to send the public key from the memory device to the smart card**, and wherein access to the user data in the memory device is enabled **upon verification that the public key and the private key are associated as a public/private key pair** such that the public and private key are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key; and
- **wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.**

With respect to Claim 7, the Patent Office repeats the rejection as stated with respect to claim 1. Accordingly, the Applicant incorporates the arguments

discusses above with respect to Claim 1 herein. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 7 be removed.

Claim 8 depends from Claim 7 and is allowable as depending from an allowable base claim. This claim is also allowable for their own recited features that, in combination with those recited in Claim 7, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claim 17 recites a method, comprising:

- storing user data and a public key on a portable memory device;
- storing a private key on a smart card;
- interfacing the smart card and the portable memory device with a computer;
- **sending the public key to the smart card**;
- verifying compatibility of the public key and the private key, wherein the verification requires that the public and private key are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key; and
- passing an encryption key, from the smart card and to the memory device, for decryption of data read from the memory device, and for encryption of data to be stored on the memory device; and
- allowing, in response to the verified compatibility, access to the user data on the portable memory device.

Claim 17 has been amended to recite, "sending the public key to the smart card," and "verifying compatibility of the public key and the private key". Accordingly, Claim 17 is allowable for at least the reasons that Claims 1 and 7 are allowable, and the arguments and remarks from above are incorporated herein, as well as the remarks associated with the traversal of the rejection of Claims 18 and

19. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 17 be removed.

Claims 4, 5, 11 and 15 are rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view Vanstone, and further in view of of U.S. Patent No. 6,353,885, hereinafter "Herzi." The Applicants respectfully traverse the rejection and request that the rejection be reconsidered and withdrawn.

Rejections to **Claim 4** were addressed, above, in relation to its independent claim 1, Claim 1.

Claim 5 recites a profile carrier comprising:

- a smart card to store a passcode and a private key from a private/public key pair; and
- a memory device to store a user profile and a public key from the private/public key pair;
- wherein, when the smart card and the memory device are interfaced with a common computing unit, the smart card is configured to permit use of the private key following validation of a user-entered passcode with the stored passcode and to authenticate, using the private key, **the public key sent to the smart card from the memory device**, wherein the authentication requires that the public and private key are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key;
- wherein the profile carrier is configured to permit access to the user profile stored on the memory device upon successful authentication of the public key at the smart card; and
- wherein the smart card is configured to pass an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Claim 5 has been amended to recite, with respect to the authentication, "the public key sent to the smart card from the memory device". Accordingly, Claim 5 is allowable for at least the reasons that Claims 1, 7 and 17 are allowable, and the

arguments and remarks from above are incorporated herein, as well as the remarks associated with the traversal of the rejection of Claims 18 and 19. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 5 be removed.

The Patent Office additionally cites the Herzi reference. However, the Herzi reference is cited for application to aspects of accessing the user's profile stored on the memory device. The Patent Office does not assert that the Herzi reference teaches or suggests aspects of authenticating, using the private key, the public key sent to the smart card from the memory device. Moreover, a careful reading of Herzi suggests that Herzi does not remedy the failings of Jones and Vanstone to teach and/or suggest a profile carrier wherein, "the public key (is) sent to the smart card from the memory device". In view of these arguments, the Applicant respectfully requests that the rejection of Claim 5 be removed.

Claim 6 depends from Claim 5 and is allowable as depending from an allowable base claim. This claim is also allowable for their own recited features that, in combination with those recited in Claim 5, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claim 11 recites a profile carrier comprising, in part, "wherein the IC card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key **and to authenticate the public key sent from the memory device to the IC card**, wherein the authentication requires confirmation that the public and private key are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key". Accordingly, Claim 11 is allowable for at least

the reasons that Claims 1, 7 and 17 are allowable, and in particular, for the reasons that Claim 5 is allowable. Accordingly, all of the arguments and remarks from above are incorporated herein, as well as the remarks associated with the traversal of the rejection of Claims 18 and 19. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 11 be removed.

Claim 12 depends from Claim 11 and is allowable as depending from an allowable base claim. This claim is also allowable for their own recited features that, in combination with those recited in Claim 11, are neither disclosed nor suggested in references of record, either singly or in combination with one another.

Claim 15 recites a method for porting a user profile for a computer, comprising:

- storing a user profile in memory of a smart card secured profile carrier, the smart card secured profile carrier having a smart card that selectively enables access to the user profile in the memory;
- interfacing the smart card secured profile carrier with the computer;
- sending a public key, stored in the memory, to the smart card;
- **verifying that a private key, stored on the smart card, is associated with the public key, received from the memory, as a public/private key pair,** wherein the association requires that the public and private key are components of an asymmetric cryptographic system whereby data encrypted by the public key may be decrypted by the private key, and wherein the public key is stored within the memory and sent to the smart card to facilitate the verifying; and
- reading the user profile from the memory, upon a successful verification, for use in configuring the computer.
- passing an encryption key to the memory device for decryption of data read from the memory device, and for encryption of data to be stored on the memory device.

Claim 15 has been amended to recite, "verifying that a private key, stored on the smart card, is associated with the public key, received from the memory, as a public/private key pair". Accordingly, Claim 15 is allowable for at least the reasons that Claims 1, 5, 7, 11 and 17 are allowable, and the arguments and remarks from above are incorporated herein, as well as the remarks associated with the traversal of the rejection of Claims 18 and 19. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 15 be removed.

The Patent Office additionally cites the Herzi reference. However, as discussed with respect to the rejection of Claim 5, the Herzi reference fails to remedy the failings of Jones and Vanstone. In view of these arguments, the Applicant respectfully requests that the rejection of Claim 15 be removed.

Claims 18 and 19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Jones in view Vanstone, and further in view of U.S. Patent No. 6,266,416, hereinafter "Sigbjornsen." The Applicants respectfully traverse the rejection and request that the rejection be reconsidered and withdrawn.

Claims 18 and 19 recite, among other aspects, "passing the public key from the memory device to the smart card" and "sending a public key from the memory to the smart card", respectively. Accordingly, Claims 18 and 19 are allowable over Jones and Vanstone for at least the reasons that Claims 1, 5, 7, 11, 15 and 17 are allowable, and the arguments and remarks from above are incorporated herein.

The Patent Office additionally cites the Sigbjornsen reference. The Sigbjornsen reference discloses a modified version of RSA cryptograph at column 7, lines 35—49. Sigbjornsen discloses use of a smart card with an embedded private key (column 7, lines 39—42). Additionally, Sigbjornsen teaches transfer

of "an un-symmetric, encrypted authentication key" to the smart card. However, this key transferred to the smart card is not actually a public key, as recited by the claim.

Sigbjornsen does not teach or suggest *sending a public key* to the smart card. This is partly because the key sent is not public. In fact, the key sent is known *only to the software producer* (column 7, lines 38—39). Additionally, the key sent, i.e. the "public key," is not a public key *because it is encrypted*, to maintain its secrecy (column 7, line 45). Thus, Sigbjornsen actually teaches an extension of RSA technology having *two private keys*. In particular, a first key is a card-embedded private key and a second key is encrypted key known only to the software vendor. Accordingly, Sigbjornsen does not disclose, "sending a public key to a smart card".

Claims 18 and 19 additionally recite, among other aspects, "authenticating, at the smart card, the public key using the private key" and "authenticating the public key using the private key", respectively. Sigbjornsen fails to teach or suggest authenticating, at the smart card, the public key using the private key. Such authentication confirms that the public key and the private key are associated as a public/private key pair, e.g. what is encrypted by the public key can be decrypted by the private key.

Referring again to Sigbjornsen at column 7, lines 44—49, an un-symmetric key is transferred to a smart card in an encrypted state (lines 44—45). Sigbjornsen then teaches that the encrypted un-symmetric key can be decrypted using a public key. That is, the private key is used to decrypt the encrypted asymmetric key. This decryption initiates the authentication process on the smart card, wherein the software (*not the public key*) is authenticated. Referring to column 8, lines 8—23,

Sigbjornsen teaches that the table seen may also be decrypted and used as a guide to software authentication.

Thus, instead of *authenticating* the public key using the private key, Sigbjornsen teaches that the encrypted public key can be *decrypted* by the private key (see column 7, lines 45—50), thereby arriving at an un-encrypted public key. In a second version, Sigbjornsen teaches that the authentication key can be encrypted, together with an identification number and the information seen in the table, and sent to the smart card (column 8, lines 5—23). Thus, decryption on the smart card reveals the authentication key and the authentication table, which instructs which private key to use in different instances.

In spite of the above teachings, Sigbjornsen fails to teach or suggest, "authenticating, at the smart card, the public key using the private key" and "authenticating the public key using the private key", as recited by Claims 18 and 19, respectively.

The Patent Office cites Sigbjornsen as teaching a system where an asymmetric authentication key is transferred to the smart card and decrypted in the smart card to initiate an authentication sequence. The Applicant respectfully disagrees that Sigbjornsen teaches or suggests the recited claim.

In particular, Sigbjornsen teaches that an un-symmetric key in an encrypted state is transferred to the smart card, where it is decrypted by a private key (Sigbjornsen at column 7, lines 45—50). Once decrypted, the process of authentication of the software (not the public key) is initiated. If additional data is also encrypted with the key (e.g. the table at column 8, lines 15—23) then that data can also be used in the authentication process.

While Sigbjornsen teaches decrypting an encrypted un-symmetric key with a private key, the disclosure made by Sigbjornsen does not teach or suggest, "authenticating the public key using the private key". Instead, Sigbjornsen's decrypting of the encrypted key simply results in the production of the decrypted key. Accordingly, the key used in the decryption is compatible with the key used to encrypt the key—not with the key that was decrypted, and which was sent to the smart card. In contrast, the Applicant's claim recited authenticating of the public key with the private key, and confirms (or denies) the compatibility of the two keys.

Thus, Sigbjornsen decrypts the key that was sent to the smart card using a private key, but fails to authenticate, or verify an association between, the key sent to the smart card and the private key embedded within the smart card. Therefore, Sigbjornsen does not fairly teach or suggest "sending a public key from the memory to the smart card; (and) authenticating the public key using the private key, thereby confirming that the public key and the private key are a public/private key pair" as recited by the Applicant's claims, as amended. Accordingly, the Applicant respectfully requests that the Patent Office remove the rejection on Claims 18 and 19.

Conclusion

Claims 1 and 3—8, 11—12, 15—19 are in believed to be in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the present application. Should any issue remain that prevents immediate issuance of the application, the Examiner is encouraged to contact the undersigned attorney to discuss the unresolved issue.

Respectfully Submitted,
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Dated: 13 April 2006 By: David S. Thompson

David S. Thompson
Reg. No. 37,954
Attorney for Applicant

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201
Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979